Math 418: Abstract algebra II.

- Handout syllabus and survey. Introduce self.

Course Overview:

1. "Nice" rings and factorization.

<u>Ring</u>: Set R with $+, \times$ [$(R,+)$ is a gp, $\times$ is assoc + dist.]

Suppose R is commutative, has 1, no zero divisors.

<u>Ex</u>: $\mathbb{Z}, \mathbb{R}, \mathbb{Z}[x], \dots$ [Query for more]

$$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

$$\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\} \subseteq \mathbb{R}$$

Any $n \in \mathbb{Z}$ can be written $n = (\pm 1)\underbrace{p_1 \cdots p_k}_{\text{primes}}$

Units: elts of R with mult. inverses.

Irreducible: if $r = a \cdot b$ then one of a, b is a unit.

[Only if asked: also a notion of prime elt: $r \mid a \cdot b \Rightarrow r \mid a$ or $r \mid b$]

<u>Unique factorization</u>: Any $r \in R$ is $= r_1 \cdot r_2 \cdots r_k$ where r_i are irreducible, in an essentially unique way.

Ex: $R = \mathbb{Z}$. $6 = 2\cdot 3 = 3 \cdot 2 = (-2)(-3) = (-3)(-2)$

Fun Facts: $\mathbb{Z}[i]$ has unique factorization, but
$\mathbb{Z}[\sqrt{5}i] = \mathbb{Z}[\sqrt{-5}]$ does not!

$$6 = \underbrace{2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})}_{\text{all irred by HW \#1.}} = 1+5 = 6$$

Motivation: Many facts about number theory can be understood in terms of factoring in such rings.

Thm: An odd prime $p \in \mathbb{Z}$ is $= a^2+b^2$ (for $a,b \in \mathbb{Z}$) iff $p \equiv 1 \bmod 4$.

[Known to ancient Greeks but "best" understood via factoring in $\mathbb{Z}[i]$; will explain in lecture 4.]

First two weeks: Euclidean domains $\Rightarrow$ Principle Ideal Domains $\Rightarrow$ Unique factorization.

Aside: Can restore unique factorization by using "ideal numbers", i.e. ideals $I \subseteq R$. ~~[illegible]~~

Introduced to study:

Fermat's Last Thm (Wiles 1990s)

$a^n + b^n = c^n$ has no solutions for $a, b, c \in \mathbb{Z}$ nonzero and $n \geq 3$.

2 Galois Theory: Study of field extensions $\overbrace{F \subseteq K}^{\text{both fields}}$.

Ex: $\mathbb{R} \subseteq \mathbb{C}$, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{R}$

algebraic extension, adding the root of a polynomial.

Focus of Galois theory

$\mathbb{Q} \subseteq \mathbb{Q}(\pi)$

Trancendental extension

An algebraic extension has an associated finite group $Gal(K/F)$. For example, $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. When K/F is Galois (whatever that means) then subfields $F \subseteq L \subseteq K$ correspond to subgroups of $Gal(K/F)$.

Query: How many subgroups does $(\mathbb{Z}/2\mathbb{Z})^2$ have?

Ans: 5

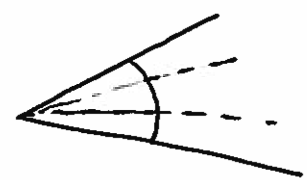
Compare:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{6}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Much of finite group theory was developed to study Galois groups.

Applications: ⓐ Unsolvability of the general quintic by radicals

ⓑ Can't trisect an angle.



③ Algebraic geometry: Study of solutions to systems of polynomial equations: $(x, y, z) \in \mathbb{C}^3$

sat $\quad x^2 + y = 1 \qquad xz + yx = 3$

Go over syllabus.